مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
سال پنجم، شماره ۲، تابستان ۱۳۹۶، ص ۴۶- ۳۷

رمزنگاری چند تصویری به‌وسیله شبکه‌های تصادفی

جواد وحیدی[1*]، روزبه متولی[2]

۱- استادیار، دانشگاه علم و صنعت ایران، ۲- کارشناس ارشد، دانشگاه آزاد اسلامی واحد ساری

(دریافت: ۹۴/۱۰/۱۶، پذیرش: ۹۵/۰۸/۱۰)

چکیده

یک شبکه تصادفی، آرایه‌ای دو بعدی از پیکسل‌ها می‌باشد. هر پیکسل در یک شبکه تصادفی یا کاملاً شفاف و یا کاملاً مات است. تعیین شفاف یا مات‌بودن پیکسل‌های یک شبکه تصادفی در یک فرآیند کاملاً تصادفی انجام می‌شود. در این مقاله یک روش جدید برای رمزنگاری چندتصویری مبتنی بر شبکه‌های تصادفی ارائه شده است. در روش ارائه شده، سه تصویر باینری تنها توسط دو شبکه تصادفی رمزگذاری می‌گردند به‌طوری‌که هر یک از شبکه‌های تصادفی به تنهایی هیچ‌گونه اطلاعاتی از تصاویر رمزگذاری‌شده در اختیار مهاجم قرار نمی‌دهند. تنها زمانی‌که هر دو شبکه تصادفی در دسترس باشند، تصاویر باینری قابل رمزگشایی و بازسازی هستند. فرآیند رمزگشایی در روش پیشنهادی با استفاده از عملگر XOR انجام می‌شود. نتایج به‌دست‌آمده از پیاده‌سازی روش پیشنهادی نشان داد که تصاویر بازسازی‌شده از کیفیت بصری بالاتری نسبت به روش‌های مشابه دیگر برخوردار هستند.

واژه‌های کلیدی: رمزنگاری، رمزنگاری چند تصویری، شبکه‌های تصادفی، کیفیت بصری

۱- مقدمه

با توجه به کاربرد روزافزون کامپیوتر، حفظ امنیت و تأیید صحت تصاویر روز به روز اهمیت بیش‌تری می‌یابد. بسیاری از سرویس‌های دیجیتالی نیازمند یک سطح امنیتی قابل قبول برای ذخیره‌سازی و انتقال تصاویر دیجیتالی می‌باشند. امروزه با رشد سریع اینترنت و شبکه‌های کامپیوتری در دنیای دیجیتال، امنیت تصاویر دیجیتالی بیش از پیش مورد توجه قرار گرفته است. روش‌های مختلفی برای مقابله با تهدیدات موجود در شبکه‌های ناامن برای دسترسی غیرمجاز به تصاویر دیجیتالی تاکنون ارائه شده‌اند که رمزنگاری تصاویر دیجیتالی مبتنی بر شمای تسهیم راز بصری یکی از موفق‌ترین و پرکاربردترین این روش‌ها بوده است. رمزنگاری تصویر مبتنی بر شمای تسهیم راز بصری به دو دسته اصلی رمزنگاری بصری و شبکه‌های تصادفی تقسیم می‌گردد.

ایده اصلی رمزنگاری تصاویر دیجیتالی بر پایه شمای تسهیم راز بصری اولین بار در سال ۱۹۸۷ توسط کافری و کرن با عنوان شبکه‌های تصادفی ارائه گردید [۱]. در روش آن‌ها، یک تصویر باینری به‌وسیله دو شبکه تصادفی مستقل از یکدیگر به گونه‌ای رمزگذاری شد که هیچ‌کدام از این شبکه‌های تصادفی به تنهایی اطلاعاتی از تصویر اصلی در اختیار مهاجم قرار نمی‌داد.

در این نوع رمزنگاری، تنها زمانی‌که دو شبکه تصادفی بر روی یکدیگر قرار گیرند، تصویر اصلی در یک پس‌زمینه تصادفی قابل رویت خواهد بود. مزیت اصلی رمزنگاری تصاویر دیجیتالی به‌وسیله شبکه‌های تصادفی آن است که فرآیند رمزگشایی نیازمند هیچ‌گونه محاسبات ریاضی نمی‌باشد و این فرآیند توسط سیستم بصری انسان صورت می‌پذیرد.

ناوور و شامیر در سال ۱۹۹۵، یک روش جدید برای رمزنگاری تصاویر دیجیتالی مبتنی بر شمای تسهیم راز بصری با عنوان رمزنگاری بصری ارائه نمودند [۲]. در روش ارائه شده توسط آن‌ها، یک تصویر باینری توسط دو سهم رمزگذاری گردید که هر یک از این سهم‌ها اطلاعاتی از تصویر رمزشده در اختیار مهاجم قرار نمی‌داد. به‌منظور بازسازی تصویر رمزشده، این دو سهم باید بر روی یکدیگر قرار می‌گرفتند. رمزنگاری بصری در مقایسه با شبکه‌های تصادفی، دارای دو مشکل اساسی است. مشکل اول آن است که اندازه تصویر بازسازی‌شده بزرگ‌تر از اندازه تصویر اصلی می‌باشد و هم‌چنین مشکل دوم آن است که اجرای فرآیند رمزگذاری در رمزنگاری بصری نیاز به کتاب کد دارد. به‌منظور مطالعه بیش‌تر درخصوص رمزنگاری بصری، می‌توان به مقالات [۶-۳] مراجعه نمود.

* رایانامه نویسنده مسئول: jvahidi@iust.ac.ir

با توجه به مزایای ذکرشده برای رمزنگاری تصاویر دیجیتالی مبتنی بر شبکه‌های تصادفی، در این مقاله یک روش جدید برای رمزنگاری چندتصویری مبتنی بر شبکه‌های تصادفی ارائه خواهد شد. در روش پیشنهادی سه تصویر باینری مختلف تنها توسط دو شبکه تصادفی رمزگذاری می‌گردند. هریک از شبکه‌های تصادفی تولیدشده به تنهایی اطلاعاتی از تصاویر رمزشده در اختیار مهاجم قرار نمی‌دهند. تنها زمانی‌که هر دو شبکه تصادفی در اختیار باشند، سه تصویر باینری مورد نظر، قابل بازسازی و رمزگشایی هستند. مزیت روش رمزنگاری پیشنهادی در مقایسه با سایر کارهای انجام‌شده در زمینه رمزنگاری تصویر مبتنی بر شبکه‌های تصادفی آن است که علاوه‌بر ویژگی رمزنگاری چندتصویری، کیفیت تصاویر بازسازی‌شده نیز بدون کم و کاست خواهد بود.

ساختار مقاله بدین صورت بیان شده است: پس از مقدمه، در بخش دوم، شبکه‌های تصادفی معرفی شده است. در بخش سوم مروری بر کارهای انجام شده بیان شده است. در بخش چهارم، روش رمزنگاری پیشنهادی معرفی گردیده و در بخش پنجم، تحلیل روش پیشنهادی و مقایسه آن با سایر روش‌ها بیان شده است. در نهایت در بخش ششم، نتیجه‌گیری ارائه شده است.

۲- شبکه‌های تصادفی

یک شبکه تصادفی، یک آرایه دوبعدی از پیکسل‌ها می‌باشد. هر پیکسل در یک شبکه تصادفی یا کاملاً شفاف و یا کاملاً مات است. تعیین شفاف یا مات‌بودن پیکسل‌های یک شبکه تصادفی در یک فرآیند شیر یا خط انجام گردیده است. بنابراین، هیچ‌گونه هم‌بستگی بین مقادیر پیکسل‌های مختلف در آرایه وجود ندارد. درنتیجه، احتمال شفاف و مات‌بودن پیکسل‌ها در شبکه تصادفی با یکدیگر برابر است. فرض کنید R نشان‌دهنده یک شبکه تصادفی باشد. میانگین درجه روشنایی شبکه تصادفی R را با T(R) نمایش می‌دهند. با توجه به احتمال یکسان برای شفاف و یا مات‌بودن پیکسل‌ها، میانگین درجه روشنایی در شبکه‌های تصادفی برابر با ۰/۵ می‌باشد [۷].

$$T(R)=0.5 \quad (۱)$$

فرض کنید $\otimes$ نشان‌دهنده عملیات OR بر روی دو شبکه تصادفی R_1 و R_2 باشد. این دو شبکه تصادفی مستقل از یکدیگر و با اندازه‌های مساوی هستند. زمانی‌که این دو شبکه تصادفی بر روی یکدیگر قرار می‌گیرند، هر پیکسل از شبکه تصادفی R_1 با یک پیکسل از شبکه تصادفی R_2 متناظر خواهد بود. جدول (۱) نتایج حاصل از روی هم قرارگیری دو پیکسل متناظر در دو شبکه تصادفی R_1 و R_2 را بر پایه عملیات OR نشان می‌دهد [۷].

جدول (۱): عملیات OR

$r_1 \in R_1$	$r_2 \in R_2$	$r_1 \otimes r_2$
□	□	□
□	■	■
■	□	■
■	■	■

با توجه به نتایج به‌دست آمده از جدول (۱)، واضح است که تنها یک برآیند از چهار حالت ممکن شفاف می‌باشد. بنابراین، میانگین درجه روشنایی $R_1 \otimes R_2$ برابر با ۱/۴ خواهد بود.

$$T(R_1 \otimes R_2)=\frac{1}{4} \quad (۲)$$

اگر $\oplus$ نشان‌دهنده عملیات XOR باشد، $R_1 \oplus R_2$ نشان‌دهنده عملیات XOR بر روی دو شبکه تصادفی مستقل از هم R_1 و R_2 خواهد بود. نتایج عملیات XOR بر روی دو پیکسل متناظر از شبکه‌های تصادفی R_1 و R_2 در جدول (۲) نشان داده شده است. با توجه به نتایج به‌دست آمده از جدول، واضح است که تنها دو برآیند از چهار حالت ممکن شفاف می‌باشند. به‌عبارت دیگر، اگر دو پیکسل متناظر هم ارزش باشند، عملیات XOR آن‌ها شفاف خواهد بود [۸].

جدول (۲): عملیات XOR

$r_1 \in R_1$	$r_2 \in R_2$	$r_1 \oplus r_2$
□	□	□
□	■	■
■	□	■
■	■	□

همان‌طورکه مشخص است، با توجه به تعداد حالات شفاف‌بودن عملیات XOR، میانگین درجه روشنایی $R_1 \oplus R_2$ برابر با ۰/۵ خواهد بود که در رابطه شماره (۳) نشان داده شده است.

$$T(R_1 \oplus R_2)=0.5 \quad (۳)$$

متمم یک شبکه تصادفی مانند R با $\bar{R}$ نشان داده می‌شود، اگر و تنها اگر برای هر دو پیکسل متناظر r و $\bar{r}$ اگر r دارای ارزش صفر باشد، $\bar{r}$ دارای ارزش یک خواهد بود و اگر r دارای ارزش یک باشد، $\bar{r}$ دارای ارزش صفر خواهد بود که با توجه به این مسئله، روابط شماره ۶-۴ برقرار خواهند بود [۷].

$$T(\bar{R})=0.5 \quad (۴)$$

$$T(R \otimes \bar{R})=0 \quad (۵)$$

$$T(R \oplus \bar{R})=0 \quad (۶)$$

نکته قابل توجه دیگر درخصوص شبکه‌های تصادفی، قانون ترکیب می‌باشد [۷]. فرض کنید X و Y دو شبکه تصادفی با ابعاد یکسان باشند. اگر A را به‌عنوان قسمتی از شبکه تصادفی X و B را به‌عنوان قسمتی از شبکه تصادفی Y در نظر بگیرید که دارای ابعاد و شکل یکسانی هستند، براساس قانون ترکیب، با جابه‌جا نمودن دو قسمت A و B در دو شبکه تصادفی X و Y، این دو شبکه تصادفی باقی خواهند ماند. در واقع، براساس قانون ترکیب، می‌توان عنوان داشت که هر زیر بخش از یک شبکه تصادفی خود یک شبکه تصادفی بوده و میانگین درجه روشنایی آن برابر با ۰/۵ خواهد بود.

۳- کارهای مرتبط

در این بخش، الگوریتم‌های مختلفی که به‌منظور رمزنگاری تصاویر دیجیتالی از شبکه‌های تصادفی استفاده نموده‌اند، مورد بحث و بررسی قرار خواهند گرفت. این روش‌ها بر اساس نوع تصاویری که می‌توانند باینری، خاکستری و رنگی باشند، به سه دسته تقسیم‌بندی می‌شوند. کافری و کرن سه الگوریتم مختلف به‌منظور رمزنگاری تصاویر باینری برپایه شبکه‌های تصادفی ارائه نمودند [۱]. در الگوریتم‌های ارائه‌شده توسط کافری و کرن، یک تصویر باینری B به‌عنوان ورودی الگوریتم پذیرفته شده و پس از اجرای فرآیند رمزگذاری، دو شبکه تصادفی R_1 و R_2 به‌عنوان خروجی الگوریتم، تولید می‌شوند. این دو شبکه تصادفی به تنهایی اطلاعاتی از تصویر باینری B در اختیار مهاجم قرار نمی‌دهند. کافری و کرن به‌منظور اجرای عملیات رمزگشایی از عملیات OR در الگوریتم‌های خود استفاده نمودند. در ادامه سه الگوریتم ارائه‌شده توسط کافری و کرن معرفی خواهند شد.

در سال ۲۰۰۷، شیو براساس الگوریتم‌های معرفی‌شده توسط کافری و کرن، روشی را برای رمزنگاری تصاویر خاکستری و رنگی ارائه نمود [۹]. در روش ارائه‌شده توسط شیو، برای رمزنگاری تصاویر خاکستری، در ابتدا تصویر خاکستری توسط الگوریتم خطای پخشی به تصویر باینری معادل تبدیل شد و سپس از سه الگوریتم کافری و کرن به‌منظور رمزنگاری تصویر باینری به‌دست‌آمده استفاده گردید. هم‌چنین به‌منظور رمزنگاری تصاویر رنگی، در ابتدا شیو تصویر رنگی را به مولفه‌های رنگی آن تجزیه نمود و سپس هر یک از مولفه‌های رنگی توسط الگوریتم ارائه‌شده برای رمزنگاری تصاویر خاکستری، به‌صورت مجزا رمزگذاری شد.

در واقع ایده اصلی روش ارائه‌شده توسط شیو برای رمزنگاری تصاویر خاکستری و رنگی، استفاده از تکنیک سایه‌انداز بوده است. الگوریتم‌های ۴ و ۵، روش‌های ارائه‌شده توسط شیو برای رمزنگاری تصاویر خاکستری و رنگی را نشان می‌دهد.

Algorithm 1

Encryption process
1. Generate R_1 as Random Grid, $T(R_1)=\frac{1}{2}$
\\ for (each pixel $R_1[i,j]$, $1\le i\le w$, $1\le j\le h$) do
\\ $R_1[i,j]$=Random_pixel(0,1)
2. for (each pixel $B[i,j]$, $1\le i\le w$, $1\le j\le h$) do
{ if($B[i,j]$==0)
$R_2[i,j]=R_1[i,j]$
else $R_2[i,j]=\overline{R_1[i,j]}$
}
3. Output(R_1,R_2)
Decryption process
1. $R_1 \otimes R_2$

الگوریتم ۱: روش اول کافری و کرن

Algorithm 2

Encryption process
1. Generate R_1 as Random Grid, $T(R_1)=\frac{1}{2}$
2. for (each pixel $B[i,j]$, $1\le i\le w$, $1\le j\le h$) do
{ if($B[i,j]$==0)
$R_2[i,j]=R_1[i,j]$
else $R_2[i,j]$=Random_pixel(0,1)
}
3. Output(R_1,R_2)
Decryption process
1. $R_1 \otimes R_2$

الگوریتم ۲: روش دوم کافری و کرن

Algorithm 3

Encryption process
1. Generate R_1 as Random Grid, $T(R_1)=\frac{1}{2}$
2. for (each pixel $B[i,j]$, $1\le i\le w$, $1\le j\le h$) do
{ if($B[i,j]$==0)
$R_2[i,j]$=Random_pixel(0,1)
else $R_2[i,j]=\overline{R_1[i,j]}$
}
3. Output(R_1,R_2)
Decryption process
1. $R_1 \otimes R_2$

الگوریتم ۳: روش سوم کافری و کرن

Algorithm 4

Input: Gray-Scale secret image G
Encryption process
1. H=Halftone (G) // error diffusion algorithm
2. Generate R_1 randomly // $R_1[i, j]$ = Random-pixel(0,1)
3. Generate R_2 by R_1 and H as follows
Based on algorithm 1 or 2 or 3
4. Output (R_1 ,R_2)
Decryption Process
1. $R_1 \otimes R_2$

الگوریتم ۴: روش شیو برای رمزنگاری تصاویر خاکستری

Algorithm 5

Input: Color secret image C in subtractive model
Encryption process
1. Decompose C into Cy, Cm and Cc,
2. Encryption Cy by algorithm 4 // Generate R_1^y and R_2^y
3. Encryption Cm by algorithm 4 // Generate R_1^m and R_2^m
4. Encryption Cc by algorithm 4 // Generate R_1^c and R_2^c
5. R_1= Combine(R_1^y, R_1^m , R_1^c)
6. R_2= Combine(R_2^y, R_2^m , R_2^c)
7.Output (R_1 ,R_2)
Decryption Process
1. $R_1 \otimes R_2$

الگوریتم ۵: روش شیو برای رمزنگاری تصاویر رنگی

هم‌چنین در سال ۲۰۰۹ شیو یک روش دیگری برای رمزنگاری تصاویر دیجیتالی مبتنی بر شبکه‌های تصادفی چندگانه ارائه نمود [۷]. در این روش، یک تصویر دیجیتالی به‌وسیله N شبکه تصادفی رمزگذاری می‌شود به‌طوری‌که هر یک از شبکه‌های تصادفی به تنهایی اطلاعاتی از تصویر رمزشده در اختیار مخاطب قرار نمی‌دهد. تنها زمانی‌که تمامی N شبکه تصادفی در دسترس باشند، تصویر بازسازی‌شده به‌صورت بصری قابل مشاهده است. بنابراین، برای اجرای فرآیند رمزگشایی به تمامی شبکه‌های تصادفی نیاز خواهد بود.

هرچند الگوریتم‌های ارائه‌شده توسط کافری و کرن از سطح امنیتی بالایی برخوردار هستند و هم‌چنین از نظر محاسبات ریاضی کم‌هزینه می‌باشند، ولیکن تصویر بازسازی‌شده در این الگوریتم‌ها از کیفیت بصری مطلوبی برخوردار نمی‌باشند. با توجه به این نقطه ضعف در روش ارائه‌شده توسط کافری و کرن، در سال ۲۰۱۲ کومار و شارما از عملگر XOR به‌منظور بازسازی تصویر اولیه در فرآیند رمزگشایی استفاده نمودند [۸]. در واقع، فرآیند رمزگذاری روش کومار و شارما دقیقاً مشابه با الگوریتم‌های کافری و کرن بوده و تنها تفاوت آن تغییر در فرآیند رمزگشایی است. نکته بسیار مهم آن است که اعمال تغییر در فاز رمزگشایی الگوریتم‌های کافری و کرن، تاثیری بر فاکتور امنیتی این الگوریتم‌ها نخواهد داشت. الگوریتم ۶، روش ارائه‌شده توسط کومار و شارما را نشان می‌دهد.

Algorithm 6

Input: Binary secret image B
Encryption process
1. Generate R_1 randomly // $R_1[i, j]$ = Random-pixel
2. Generate R_2 by R_1 and B as follows
   Based on algorithm 1 or 2 or 3
3. Output (R_1 ,R_2)
Decryption Process
1. $R_1 \oplus R_2$

الگوریتم ۶: روش ارائه‌شده توسط کومار و شارما

در سال ۲۰۱۲، چن و لی یک روش جدیدی برای رمزنگاری چندتصویری مبتنی بر شبکه‌ها تصادفی ارائه نمودند [۱۰]. در روش ارائه‌شده توسط آن‌ها، چند تصویر باینری به‌صورت هم‌زمان توسط دو شبکه تصادفی مدور رمزنگاری می‌شود. هر پیکسل از تصویر باینری با یک سکتور[1] در شبکه تصادفی مدور ارتباط دارد. روند کار بدین صورت است که در گام اول، تصویر باینری به شکل یک آرایه تک‌بعدی درنظر گرفته می‌شود. در گام دوم، شبکه تصادفی مدور اول به‌صورت کاملاً تصادفی تولید می‌گردد. سپس در گام سوم با استفاده از رویکرد تعریف‌شده، شبکه تصادفی مدور دوم براساس تصویر باینری و شبکه تصادفی مدور اول، تولید می‌شود. برای رمزنگاری تصاویر باینری بعدی کافی است که یکی از دو شبکه تصادفی براساس فاکتوری از تعداد تصاویر چرخانده شود.

در سال ۲۰۱۵، وحیدی و همکارانش، یک روش جدیدی برای رمزنگاری تصاویر خاکستری مبتنی بر شبکه‌های تصادفی ارائه نمودند [۱۱]. در روش ارائه شده توسط آن‌ها، از روش سطح بیت برای رمزنگاری تصویر خاکستری بهره گرفته شده است. روش کار بدین صورت است که در ابتدا تصویر خاکستری مورد نظر توسط روش سطح بیت، به هشت سطح بیت معادل تبدیل می‌شود. سپس سه سطح بیت با ارزش تصویر توسط الگوریتم شماره یک رمزگذاری می‌شوند. شش شبکه تصادفی حاصل‌شده، با یکدیگر ترکیب و درنهایت دو شبکه تصادفی نهایی را تولید می‌نمایند. با اجرای عملیات XOR بر روی این دو شبکه تصادفی نهایی، تصویر اصلی بازسازی می‌شود. نکته قابل توجه در این روش آن است که تصویر بازسازی‌شده، خود یک تصویر خاکستری بوده و از کیفیت بصری بالایی برخوردار می‌باشد. الگوریتم ۷، روش ارائه‌شده توسط وحیدی برای رمزنگاری تصاویر خاکستری را نشان می‌دهد.

Algorithm 7

Input: Gray-Scale secret image G
Encryption process
1. Decompose the gray-scale image G
2. Selected valuable bit planes \\ Bit planes 6, 7, and 8
3. Encode the valuable bit planes by algorithm 1
   \\ six random grids $R_1^6,R_2^6,R_1^7,R_2^7,R_1^8,R_2^8$
4. R_1= Combine (R_1^6,R_1^7,R_1^8)
5. R_2= Combine (R_2^6,R_2^7,R_2^8)
6. Output (R_1 , R_2)
Decryption Process
1. $R_1 \oplus R_2$

الگوریتم ۷: روش وحیدی برای رمزنگاری تصاویر خاکستری

در سال ۲۰۱۵، گورانگ و همکارانش، یک روش جدیدی برای رمزنگاری چندتصویری مبتنی بر شبکه‌های تصادفی مکعبی ارائه نمودند [۱۲]. در روش ارائه‌شده توسط آن‌ها، از نمای بیرونی شبکه‌های تصادفی مکعبی برای رمزنگاری تصاویر دیجیتالی استفاده شده است. هر نمای بیرونی یک شبکه تصادفی مکعبی می‌تواند برای رمزنگاری چهار تصویر دیجیتالی مورد استفاده قرار گیرد. نمای بیرونی از قبل تعیین‌شده دو شبکه تصادفی مکعبی به‌ترتیب با زاویه چرخش ۰، ۹۰، ۱۸۰ و ۲۷۰ درجه برای رمزنگاری چهار تصویر باینری مورد استفاده قرار می‌گیرند. در واقع، شبکه تصادفی مکعبی اول همواره ثابت بوده و شبکه

[1] Sector

تصادفی مکعبی دوم به منظور رمزگذاری و رمزگشایی تصاویر باینری چرخانده می‌شود.

اکثر روش‌های معرفی‌شده برای رمزنگاری تصاویر دیجیتالی مبتنی بر شبکه‌های تصادفی، دارای یک مشکل اساسی هستند. مشکل اصلی این دسته از روش‌ها، کیفیت پایین تصویر رمزگشایی‌شده می‌باشد. در واقع، تصویر بازسازی‌شده نسبت به تصویر اولیه از کیفیت بصری پایین‌تری برخوردار می‌باشد. برای مطالعه بیش‌تر درخصوص روش‌های رمزنگاری تصویر مبتنی بر شبکه‌های تصادفی می‌توان به مقالات [۱۵-۱۳] مراجعه نمود.

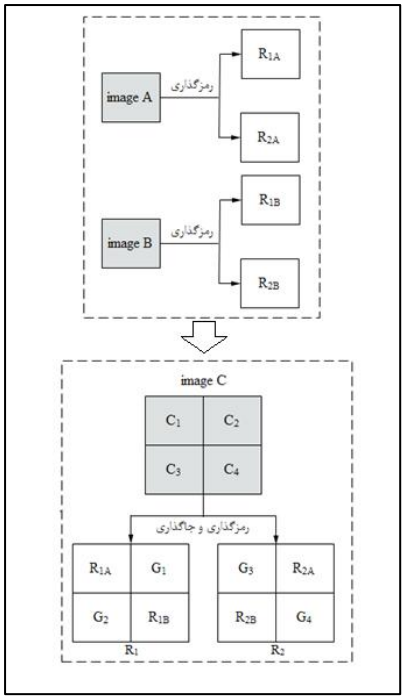
۴- روش پیشنهادی

در این بخش، یک روش جدید برای رمزنگاری چندتصویری به‌وسیله شبکه‌های تصادفی با بهره‌گیری از الگوریتم‌های کافری و کرن، ارائه خواهد شد. در روش پیشنهادی، سه تصویر باینری به‌وسیله دو شبکه تصادفی رمزگذاری می‌شوند. در واقع، در روش پیشنهادی دو تصویر با ابعاد M×M پیکسل و یک تصویر با ابعاد 2M×2M پیکسل به‌وسیله دو شبکه تصادفی، رمزگذاری می‌گردند. شبکه‌های تصادفی به‌تنهایی هیچ اطلاعاتی از سه تصویر رمزشده در اختیار مهاجم قرار نخواهند داد. تنها زمانی‌که هر دو شبکه تصادفی در دسترس باشند، می‌توان هر سه تصویر رمزشده را رمزگشایی نمود. در ادامه، مراحل رمزگذاری و رمزگشایی روش پیشنهادی معرفی شده و هم‌چنین توسعه روش پیشنهادی برای رمزنگاری تصاویر خاکستری توضیح داده خواهد شد.

۴-۱- مرحله رمزگذاری

در شکل (۱)، شمای کلی مرحله رمزگذاری نشان داده شده است. همان‌طورکه در شکل مشخص است، مرحله رمزگذاری از دو گام اصلی تشکیل شده است. در گام اول، دو تصویر باینری A و B با ابعاد برابر با یکدیگر به مجزا توسط الگوریتم ۱ کافری و کرن، رمزگذاری می‌گردند که حاصل رمزگذاری این دو تصویر، چهار شبکه تصادفی R_{1A}، R_{2A}، R_{1B} و R_{2B} می‌باشند. این چهار شبکه تصادفی به‌عنوان ورودی‌های گام دوم درنظر گرفته می‌شوند.

در گام دوم، تصویر باینری C که دارای ابعاد بزرگ‌تری است، توسط دو شبکه تصادفی R_1 و R_2 رمزگذاری می‌گردد. به‌منظور تولید دو شبکه تصادفی R_1 و R_2، در ابتدا چهار شبکه تصادفی R_{1A}، R_{2A}، R_{1B} و R_{2B} در مکان‌های مشخص‌شده در شکل جاگذاری می‌گردند. قسمت‌های باقی‌مانده در دو شبکه تصادفی R_1 و R_2 به‌ترتیب با نام‌های G_1، G_2، G_3 و G_4 نشان داده شده‌اند. به‌منظور تولید این قسمت‌ها در شبکه‌های تصادفی، از قسمت متناظر در تصویر اصلی C و قسمت متناظر در شبکه تصادفی مقابل استفاده می‌شود. به‌عنوان نمونه برای تولید قسمت G_1 از قسمت‌های C_2 و R_{2A} استفاده می‌شود.



شکل (۱): مرحله رمزگذاری

الگوریتم ۸، فاز رمزگذاری روش پیشنهادی را نشان می‌دهد. با توجه به الگوریتم طراحی‌شده، سه تصویر باینری مختلف توسط دو شبکه تصادفی، رمزگذاری می‌گردند. به‌منظور پیاده‌سازی گام اول در مرحله رمزگذاری، دو تصویر باینری ۲۵۶ × ۲۵۶ پیکسل درنظر گرفته شده‌اند. این دو تصویر باینری به‌صورت مجزا و براساس الگوریتم ۱ کافری و کرن، رمزگذاری شده‌اند.

Algorithm 8

First Step

Input: images A and B \\ with size M×M

1. Encrypt image A with algorithm 1
2. Encrypt image B with algorithm 1

Output of first step: Random grids R_{1A}, R_{2A}, R_{1B} and R_{2B}

Second Step

Input: image C and R_{1A}, R_{2A}, R_{1B}, R_{2B} \\ size C is 2M×2M

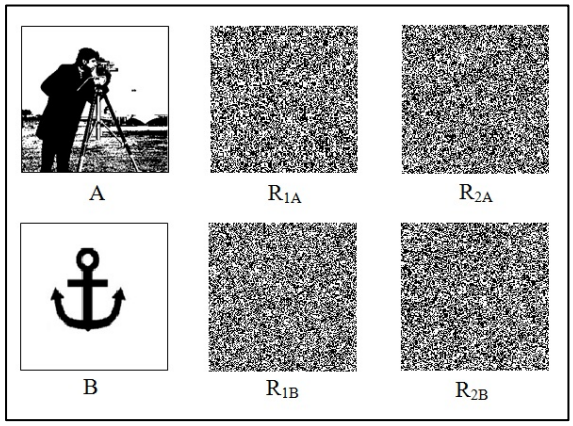
1. Put R_{1A} in first quarter of R_1
2. Put R_{1B} in fourth quarter of R_1
3. Put R_{2A} in second quarter of R_2
4. Put R_{2B} in third quarter of R_2
5. Generate G_1 based on C_2 and R_{2A}, using algorithm 1
6. Generate G_2 based on C_3 and R_{2B}, using algorithm 1
7. Generate G_3 based on C_1 and R_{1A}, using algorithm 1
8. Generate G_4 based on C_4 and R_{1B}, using algorithm 1

Output of second phase: Random grids R_1 and R_2

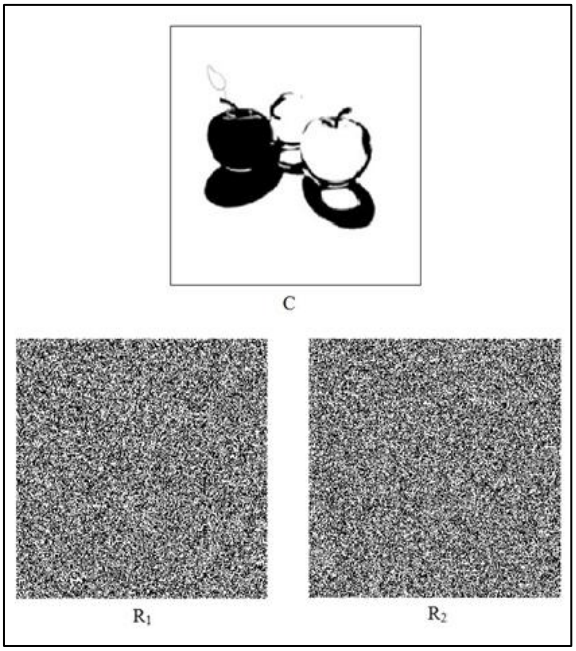
الگوریتم (۸): فاز رمزگذاری روش پیشنهادی

شکل (۲) نتایج حاصل از پیاده‌سازی گام اول در مرحله رمزگذاری را نشان می‌دهد. همان‌طورکه در شکل مشخص است، خروجی این گام، چهار شبکه تصادفی R_{1A}، R_{2A}، R_{1B} و R_{2B} خواهند بود.

برای پیاده‌سازی گام دوم در مرحله رمزگذاری، یک تصویر باینری با ابعاد ۵۱۲ × ۵۱۲ پیکسل درنظر گرفته شده است. به‌منظور رمزگذاری تصویر سوم، باید شبکه‌های تصادفی با ابعاد مساوی با آن ساخته شود. برای دست‌یابی به این هدف، از چهار شبکه تصادفی R_{1A}، R_{2A}، R_{1B} و R_{2B} و تصویر اصلی C استفاده می‌شود. شکل (۳) نتایج حاصل از پیاده‌سازی گام دوم در مرحله رمزگذاری را نشان می‌دهد. همان‌طورکه در شکل مشخص است، خروجی این گام دو شبکه تصادفی R_1 و R_2 می‌باشند.



شکل (۲): پیاده‌سازی گام اول در مرحله رمزگذاری



شکل (۳): پیاده‌سازی گام دوم در مرحله رمزگذاری

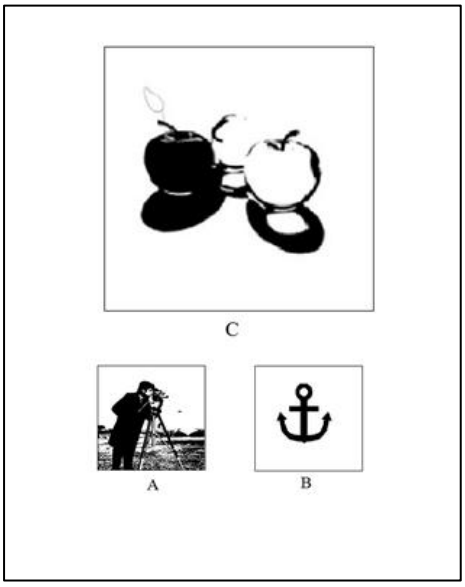
۴-۲- مرحله رمزگشایی

به‌منظور اجرای فرآیند رمزگشایی، کافی است تا شبکه‌های تصادفی متناظر با یکدیگر XOR شوند. با اعمال عملگر XOR بر روی دو شبکه تصادفی R_1 و R_2 به‌راحتی می‌توان تصویر C را بازسازی نمود. هرچند بازسازی دو تصویر A و B کمی پیچیده‌تر می‌باشد. برای بازسازی این دو تصویر، در ابتدا باید شبکه‌های تصادفی متناظر با آن‌ها از دو شبکه تصادفی R_1 و R_2 استخراج شده و سپس عملیات XOR بر روی آن‌ها اعمال گردد. الگوریتم ۹، فاز رمزگشایی روش پیشنهادی را نشان می‌دهد. همان‌طورکه مشخص است، خروجی این الگوریتم سه تصویر باینری مورد نظر می‌باشند.

Algorithm 9

Input: Random grids R_1 and R_2 \\ size 2M×2M
Decryption 1 \\ image C
  for (each pixel C[i,j], 1≤i≤2M and 1≤j≤2M) do
    C[i,j]= R_1[i,j] XOR R_2[i,j]
Decryption 2 \\ image A
  Extract R_{1A} from R_1
  Extract R_{2A} from R_2
  for (each pixel A[i,j], 1≤i≤M and 1≤j≤M) do
    A[i,j]= R_{1A}[i,j] XOR R_{2A}[i,j]
Decryption 3 \\ image B
  Extract R_{1B} from R_1
  Extract R_{2B} from R_2
  for (each pixel B[i,j], 1≤i≤M and 1≤j≤M) do
    B[i,j]= R_{1B}[i,j] XOR R_{2B}[i,j]
Outputs (image C, image A, image B)

الگوریتم ۹: فاز رمزگشایی روش پیشنهادی



شکل (۴): پیاده‌سازی مرحله رمزگشایی

در شکل (۴) نتایج حاصل از پیاده‌سازی مرحله رمزگشایی

نشان داده شده است. همان‌طورکه مشخص است، تصاویر بازسازی‌شده ازلحاظ بصری دقیقاً مشابه با تصاویر باینری اولیه می‌باشند که این مسئله به‌عنوان یک مزیت در روش رمزنگاری پیشنهادی محسوب می‌شود. در واقع، کیفیت تصاویر رمزگشایی‌شده بدون کم و کاست می‌باشد. در بخش پنج، این مسئله با استفاده از قضایای ریاضی اثبات خواهد شد.

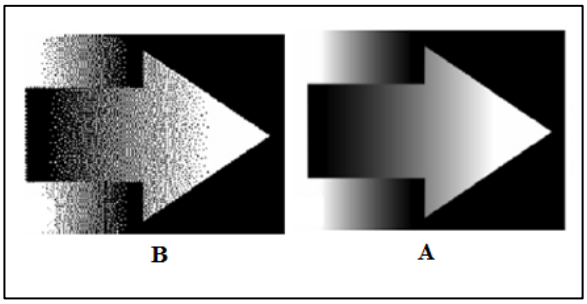
۴-۳- توسعه روش پیشنهادی

روش رمزنگاری پیشنهادی را می‌توان به‌منظور رمزنگاری تصاویر خاکستری نیز توسعه داد. ایده اصلی برای رمزنگاری سه تصویر خاکستری به‌وسیله دو شبکه تصادفی، تبدیل تصاویر خاکستری به تصاویر باینری به‌وسیله روش سایه‌انداز و بهره‌مندی از توانایی‌های به‌دست‌آمده از رمزنگاری سه تصویر باینری به‌وسیله دو شبکه تصادفی می‌باشد. روش سایه‌انداز از شبکه‌ای از نقاط باینری برای شبیه‌سازی تصاویر خاکستری استفاده می‌کند. در واقع، تصاویر سایه‌انداز شامل پیکسل‌های سیاه و سفید هستند و سیستم بصری انسان قابلیت تشخیص اطلاعات تصویر خاکستری معادل را دارد. به‌منظور تبدیل تصاویر خاکستری به تصاویر باینری معادل می‌توان از الگوریتم خطای پخشی استفاده نمود. الگوریتم ۱۰، الگوریتم خطای پخشی را نشان می‌دهد.

Algorithm 10

```
Input: Gray-Scale secret image G \\ size N×M
Output: Halftone Image H
for i=1:N
  for j=1:M
    Compute the value of  H(i , j) by Threshold level
    Error=L(i , j) – (255*H(i , j))
    L(i ,j) = L(i ,j)+(Error*(7/16))
    L(i+1 ,j-1) = L(i+1 ,j-1)+(Error*(3/16))
    L(i+1 ,j) = L(i+1 ,j)+(Error*(5/16))
    L(i+1 ,j+1) = L(i+1 ,j+1)+(Error*(1/16))
  end
end
```

الگوریتم ۱۰: الگوریتم خطای پخشی



شکل (۵): تصویر خاکستری و تصویر باینری معادل

شکل (۵) یک تصویر خاکستری و تصویر باینری معادل آن با استفاده از الگوریتم خطای پخشی را نشان می‌دهد. نکته قابل توجه آن است که کیفیت تصویر باینری معادل نسبت به کیفیت تصویر خاکستری کاهش یافته است که این مسئله با هدف تعیین‌شده در مقاله سازگاری ندارد.

۵- تحلیل روش پیشنهادی و مقایسه با سایر روش‌ها

به منظور تحلیل روش‌های رمزنگاری تصویر به‌وسیله شبکه‌های تصادفی باید دو ویژگی امنیت و کیفیت بصری مورد توجه قرار گیرد. امنیت بدین معنی است که هر یک از شبکه‌های تصادفی به تنهایی نباید باعث آشکارشدن تصویر رمزشده شوند و ویژگی کیفیت بصری نیز به معنی آن است که نتایج حاصل از روی‌هم قرارگرفتن دو شبکه تصادفی باید به‌گونه‌ای باشد تا تصویر مورد نظر توسط سیستم بصری انسان قابل تشخیص باشد. برای اثبات امنیت و کیفیت بصری یک الگوریتم رمزنگاری تصویر مبتنی بر شبکه‌های تصادفی، باید قضیه شماره ۱ اثبات گردد [۹].

قضیه ۱: در روش طراحی‌شده برای رمزنگاری چندتصویری مبتنی بر شبکه‌های تصادفی، برای دو شبکه تصادفی تولیدشده نهایی، باید روابط زیر برقرار باشند که رابطه شماره ۷ برای اثبات امنیت روش و رابطه شماره ۸ برای اثبات کیفیت بصری روش می‌باشند.

$$T(R_1)=T(R_2)=0.5 \qquad (۷)$$

$$T(S[C(0)])>T(S[C(1)]) \quad \text{where } S=R_1 \oplus R_2 \qquad (۸)$$

لم اثبات: فرض کنید که C(0) نشان‌دهنده تمام پیکسل‌های شفاف تصویر باینری C و C(1) نشان‌دهنده تمام پیکسل‌های مات تصویر باینری C باشند. در این صورت، روابط زیر برقرار خواهند بود:

$c \in C(0)$ if and only if $c=0$

$c \in C(1)$ if and only if $c=1$

$C=C(0) \cup C(1)$

$\emptyset=C(0) \cap C(1)$

همه پیکسل‌های متناظر با C(0) در شبکه تصادفی R با R[C(0)] و همه پیکسل‌های متناظر با C(1) در شبکه تصادفی R با R[C(1)] نشان داده می‌شوند. در نتیجه روابط زیر برقرار خواهند بود:

$R=R[C(0)] \cup R[C(1)]$

$\emptyset=R[C(0)] \cap R[C(1)]$

اثبات رابطه ۷: به‌منظور اثبات شرط امنیتی در الگوریتم ارائه‌شده، باید نشان دهیم که تمامی R_{1A}، R_{2A}، R_{1B}، R_{2B}، G_1، G_2، G_3 و G_4 شبکه‌های تصادفی هستند و میانگین درجه روشنایی همه آن‌ها برابر با ۰/۵ است.

از آن‌جایی‌که R_{1A} به‌صورت کاملاً تصادفی و در یک فرآیند شیر یا خط تولید شده است، در نتیجه R_{1A} یک شبکه تصادفی است و میانگین درجه روشنایی آن برابر با ۰/۵ می‌باشد. هم‌چنین، متمم شبکه تصادفی R_{1A} نیز خود یک شبکه تصادفی می‌باشد. با توجه به الگوریتم ۱ $R_{1A}[A(0)]=R_{2A}[A(0)]$ بوده و از آن‌جایی‌که R_{1A} یک شبکه تصادفی است، در نتیجه $R_{2A}[A(0)]$ یک شبکه تصادفی بوده و میانگین درجه روشنایی آن برابر با ۰/۵ است. از طرف دیگر، براساس الگوریتم ۱، $R_{2A}[A(1)]=\overline{R_{1A}[A(1)]}$ بوده و با توجه به این‌که متمم R_{1A} یک شبکه تصادفی است، بنابراین $R_{2A}[A(1)]$ یک شبکه تصادفی بوده و میانگین درجه روشنایی آن برابر با ۰/۵ است. با توجه به موارد مطرح شده داریم:

$$R_{2A}=R_{2A}[A(0)]\cup R_{2A}[A(1)]$$

$$T(R_{2A})=0.5$$

به‌صورت مشابه، می‌توان اثبات نمود که R_{1B} و R_{2B} نیز دو شبکه تصادفی هستند و میانگین درجه روشنایی آن‌ها برابر با ۰/۵ می‌باشد. تاکنون اثبات گردید که R_{1A}، R_{2A}، R_{1B} و R_{2B} شبکه‌های تصادفی می‌باشند و میانگین درجه روشنایی آن‌ها برابر با ۰/۵ است. اکنون نوبت آن است که ثابت شود G_1، G_2، G_3 و G_4 نیز شبکه‌های تصادفی هستند. در الگوریتم طراحی‌شده، به‌منظور ساخت G_1، از شبکه تصادفی R_{2A} و قسمت C_2 در تصویر اصلی استفاده شد. با توجه به این‌که R_{2A} یک شبکه تصادفی بوده و $G_1[C_2(0)]=R_{2A}[C_2(0)]$، در نتیجه $G_1[C_2(0)]$ یک شبکه تصادفی است و میانگین درجه روشنایی آن برابر با ۰/۵ می‌باشد. هم‌چنین، با توجه به این‌که $G_1[C_2(1)]=\overline{R_{2A}[C_2(1)]}$ بوده و متمم شبکه تصادفی R_{2A} خود یک شبکه تصادفی است، درنتیجه $G_1[C_2(1)]$ نیز یک شبکه تصادفی می‌باشد. با توجه به مسائل مطرح شده داریم:

$$G_1=G_1[C_2(0)]\cup G_1[C_2(1)]$$

$$T(G_1)=0.5$$

ثابت شد که G_1 یک شبکه تصادفی است و میانگین درجه روشنایی آن برابر با ۰/۵ می‌باشد. با توجه به نحوه اثبات این مسئله، به‌صورت مشابه می‌توان بیان نمود که G_2، G_3 و G_4 نیز شبکه‌های تصادفی هستند. از آن‌جایی‌که R_1 از کنار هم قرارگیری شبکه‌های تصادفی R_{1A}، R_{1B}، G_1 و G_2 تشکیل شده است، بنابراین خود یک شبکه تصادفی بوده و میانگین درجه روشنایی آن برابر با ۰/۵ خواهد بود. به همین ترتیب، می‌توان عنوان نمود که R_2 نیز یک شبکه تصادفی با میانگین درجه روشنایی ۰/۵ است. در نتیجه شرط امنیتی برای روش پیشنهادی برقرار است.

اثبات رابطه ۸: برای اثبات کیفیت بصری در روش پیشنهادی باید رابطه شماره ۸ اثبات گردد که شرط کنتراست تصویر است. به‌منظور اثبات این رابطه، باید نشان داده شود که میانگین درجه روشنایی $S[C(0)]$ بزرگ‌تر از میانگین درجه روشنایی $S[C(1)]$ است. برای اثبات این موضوع داریم:

$$S[C(0)]=R_1[C(0)]\oplus R_2[C(0)]=0$$

$$S[C(1)]=R_1[C(1)]\oplus R_2[C(1)]=1$$

$$T(S[C(0)])=1$$

$$T(S[C(1)])=0$$

بنابراین، با توجه به این‌که میانگین درجه روشنایی $S[C(0)]$ بزرگ‌تر از میانگین درجه روشنایی $S[C(1)]$ می‌باشد، شرط کیفیت بصری نیز در روش پیشنهادی برقرار است. هم‌چنین شایان ذکر است که با توجه به نتایج به‌دست‌آمده از تحلیل، اگر پیکسل تصویر اصلی سفید باشد، قطعاً پیکسل متناظر در تصویر بازسازی‌شده نیز سفید خواهد بود و اگر پیکسل تصویر اصلی سیاه باشد، قطعاً پیکسل متناظر در تصویر بازسازی‌شده نیز سیاه خواهد بود. با توجه به این نکته، تصویر بازسازی‌شده از لحاظ بصری دقیقاً مشابه با تصویر اصلی اولیه می‌باشد. به‌منظور درک بیشتر این موضوع، فرآیند کدکردن یک پیکسل مشخص از تصویر C در جدول (۳) نشان داده شده است.

جدول (۳): فرآیند کدکردن یک پیکسل مشخص

$c\in C$	احتمال وقوع	$r_1\in R_1$	$r_2\in R_2$	$r_1\oplus r_2$
□	۱/۴	□	□	□
	۱/۴	■	■	□
■	۱/۴	□	■	■
	۱/۴	■	□	■

یکی دیگر از معیارهای تحلیل و ارزیابی یک روش رمزنگاری تصویر محاسبه پیچیدگی زمانی روش می‌باشد. به‌منظور محاسبه پیچیدگی زمانی روش پیشنهادی، باید فرآیندهای رمزگذاری و

رمزگشایی را به‌صورت مجزا مورد بررسی قرار داد. در روش پیشنهادی و در مرحله رمزگذاری، مطابق با الگوریتم ۸، پیچیدگی زمانی برابر با $O(N^2)$ می‌باشد. متغیر N نشان‌دهنده اندازه ابعاد تصویر باینری C برحسب پیکسل است. همچنین در

جدول (۴): مقایسه روش پیشنهادی با سایر روش‌ها

نام روش	روش رمزنگاری	نوع تصویر	لزوم کتاب کد	گسترش پیکسل	رمزنگاری چند تصویری	کیفیت تصویر بازسازی شده
ناوور و شامیر [۲]	رمزنگاری بصری	باینری	بله	بله	خیر	با کم و کاست
کافری و کرن [۱]	شبکه‌های تصادفی	باینری	خیر	خیر	خیر	با کم و کاست
شیو [۹]	شبکه‌های تصادفی	خاکستری و رنگی	خیر	خیر	خیر	با کم و کاست
شیو [۷]	شبکه‌های تصادفی	باینری، خاکستری و رنگی	خیر	خیر	خیر	با کم و کاست
کومار و شارما [۸]	شبکه‌های تصادفی	باینری	خیر	خیر	خیر	بدون کم و کاست
چن و لی [۱۰]	شبکه‌های تصادفی	باینری	خیر	خیر	بله	با کم و کاست
وحیدی [۱۱]	شبکه‌های تصادفی	خاکستری	خیر	خیر	خیر	با کم و کاست
گورانگ [۱۲]	شبکه‌های تصادفی	باینری	خیر	خیر	بله	با کم و کاست
روش پیشنهادی	شبکه‌های تصادفی	باینری	خیر	خیر	بله	بدون کم و کاست

روش پیشنهادی برای بازیابی دو تصویر باینری A و B پیچیدگی زمانی معادل با $O(M^2)$ و برای بازیابی تصویر باینری C پیچیدگی زمانی معادل با $O(N^2)$ می‌باشد. با توجه به نکات مطرح‌شده، می‌توان عنوان داشت که پیچیدگی زمانی روش رمزنگاری پیشنهادی از مرتبه چندجمله‌ای است که نشان‌دهنده سرعت بالای روش پیشنهادی خواهد بود.

روش پیشنهادی با سایر روش‌های معرفی‌شده مورد مقایسه قرار گرفته و نتایج به‌دست آمده در جدول (۴) نشان داده شده است. همان‌طورکه از نتایج به‌دست آمده در جدول مشخص است، در روش‌های کومار و شارما [۸] و روش پیشنهادی، تصویر رمزگشایی‌شده بدون کم و کاست قابل بازسازی می‌باشد. درحالی که در مابقی روش‌های معرفی‌شده، تصویر بازسازی‌شده از لحاظ بصری از کیفیت پایین‌تری نسبت به تصویر اصلی برخوردار می‌باشد. برتری روش پیشنهادی در مقایسه با روش ارائه‌شده توسط کومار و شارما، رمزنگاری چندتصویری است. در واقع، در روش پیشنهادی به‌طور هم‌زمان سه تصویر باینری به‌وسیله دو شبکه تصادفی رمزگذاری می‌گردند، درحالی‌که در روش کومار و شارما تنها یک تصویر باینری به‌وسیله دو شبکه تصادفی رمزگذاری می‌شود.

۶- نتیجه‌گیری

همان‌طورکه گفته شد، روش رمزنگاری بصری در مقایسه با شبکه‌های تصادفی دارای دو مشکل اساسی گسترش پیکسل‌ها و نیاز به کتاب کد می‌باشد. در این مقاله تلاش شد تا یک روش جدید رمزنگاری چندتصویری مبتنی بر شبکه‌های تصادفی ارائه شود. در روش پیشنهادی، سه تصویر باینری به‌صورت هم‌زمان به‌وسیله دو شبکه تصادفی مختلف رمزگذاری شدند به‌گونه‌ای‌که هر یک از شبکه‌های تصادفی به تنهایی اطلاعاتی از تصاویر رمزشده در اختیار مهاجم قرار نمی‌دهند. تنها زمانی‌که هر دو شبکه تصادفی در اختیار ما باشد، تصاویر باینری بدون هیچ‌گونه کم و کاست، قابل بازسازی می‌باشند. هم‌چنین رویکردی برای توسعه روش پیشنهادی برای رمزنگاری تصاویر خاکستری پیشنهاد شد. روش پیشنهادی توسط نرم‌افزار متلب نسخه ۲۰۱۰ پیاده‌سازی و شرایط امنیتی و کیفیت بصری روش پیشنهادی با استفاده از قضایای ریاضی اثبات گردید. با استفاده از قضایای ریاضی اثبات شد که تصاویر بازسازی‌شده از لحاظ بصری دقیقاً مشابه با تصاویر اصلی اولیه می‌باشد که این مسئله به‌عنوان مزیت اصلی روش پیشنهادی محسوب می‌گردد.

۷- مراجع

[1] O. kafri and E. keren, “encryption of pictures and shapes by random Grids,” opt, let 12, pp. 377-379, 1987.

[2] M. Naor and A. Shamir, “Visual Cryptography,” in: A. De Santis (Ed.), Advances in Cryptology: Eurpocrypt'94, Lecture Notes in Computer Science, vol. 950, pp. 1-12, 1995.

[3] C. C. Lin and W. H. Tsai, “Visual cryptography for gray-level images by dithering techniques,” Pattern Recognition letters, vol.

24, pp. 349-358, 2003.

[4] Y. C. Hou, "Visual cryptography for color images," Pattern Recognition, vol. 36, pp. 1619-1629, 2003.

[5] A. Ross and A. Othman, "Visual Cryptography for Biometric Privacy," IEEE Transaction on Information Forensics and Security, vol. 6, no. 1, pp. 70-81, 2011.

[6] Y. E. Tetik, A. Yildizhan, and K. Erol, "Improving the perceived quality of half tone secret images in visual cryptography," 23th Conference on Signal Processing and Communications Applications, Malatya, Turkey, pp. 682-685, 2015.

[7] S. J. Shyu, "Image encryption by multiple random grids," Pattern Recognition, vol. 42, pp. 1582-1596, 2009.

[8] S. Kumar and R. K. Sharma, "Improving contrast in random grids based visual secret sharing," International journal of security and its application, vol. 6, no. 1, pp. 9-27, 2012.

[9] S. J. Shyu, "Image encryption by random grids," Pattern Recognition, vol. 40, pp. 1014-1031, 2007.

[10] T. H. Chen and K. C. Li, "Multi-image encryption by circular random grids," Information Sciences, vol. 189, pp. 255-265, 2012.

[11] J. Vahidi, M. Riyahi, and R. Motevalli, "A new approach for gray scale image encryption by random grids," International journal of mechatronics, Electrical and Computer Technology, vol. 5, no. 16, pp. 2169-2174, 2015.

[12] S. Gurung, K. P. Choudhury, A. Parmar, and K. Panghaal, "Multiple Information Hiding using Cubical Approach on Random Grids," International Journal of Computer Network and Information Security, vol. 11, pp. 54-63, 2015.

[13] T. H. Chen and K. H. Tsao, "Threshold visual secret sharing by random grids," System and Software, vol. 84, no. 7, pp. 1197-1208, 2011.

[14] T. Guo, F. Liu, and C. Wu, "Threshold visual secret sharing by random grids," System and Software, vol. 86, no. 9, pp. 2094-2109, 2013.

[15] S. J. Shyu, "Visual cryptograms of random grids for Threshold access structures," Theoretical Computer Science, vol. 569, pp. 30-49, 2015.

Journal Of Electronical & Cyber Defence
Vol. 5, No. 2, 2017, Serial No. 18

Multi-Image Encryption by Random Grids

J. Vahidi*, R. Motevalli

*Iran University of Science and Technology

(Received: 06/01/2016 , Accepted: 31/10/2016)

ABSTRACT

A random grid is a 2-dimensional array. Each pixel in random grid is either transparent or dark. Darkness and transparency of each pixel are determined by a total random process. This paper introduces a new method for multi-image encryption by random grids. In the proposed method, three binary images are encrypted by only two random grids in such a way that each random grid does not give the attacker any information. Binary images can not be decrypted and reconstructed only when two random grids are accessible. Decryption process is done by XOR operation. The result of implementation of the proposed method showed that reconstructed images have higher visual quality in comparison with previous approaches.

Keywords: Encryption, Multi Image Encryption, Random Grids, Visual Quality

* Corresponding Author Email: jvahidi@iust.ac.ir